WHAT IS CLAIMED IS:

1. In a wireless network having at least two access points (APs), each AP having a predetermined service area, and a station (STA) that receives a communication service by associating with a first AP being one of the at least two APs, a method of supporting a roaming service for the STA at the first AP, comprising the steps of:

generating an AP-neighborhood graph containing neighbor APs to which the STA can move;

acquiring proactive keys for the neighbor APs based on association information gained from the association of the STA to the first AP; and

transmitting the proactive keys to the neighbor APs by proactive caching,

whereby performing a pre-authentication such that when the STA attempts to roam to one of the neighbor APs, fast roaming is provided via a proactive key provided to the neighbor AP.

2. The method of claim 1, wherein an AP-neighborhood graph is generated at each of the at least two APs.

3. The method of claim 2, wherein the neighbor APs are APs within a distance less than a predetermined threshold, to which the STA can move from the first AP without being by way of any other AP.

4. The method of claim 1, wherein the association information includes a pairwise master key (PMK: PMK_{curr}) and a roam key (RK) which are acquired at the first AP, and the MAC addresses of the STA and the neighbor APs (STA_{mac} and next AP_{mac}), and a PMK (PMK_{next}) for each of the neighbor APs is acquired using the association information and determined by

$$PMK_{next} = PRF(RK, PMK_{curr}, STA_{mac}, \text{next } AP_{mac})$$

5. The method of claim 4, wherein the RK is determined by

$$RK = PRF(PMK, \text{“Roam Key”}, AP_{nonce}, STA_{nonce})$$

where AP_{nonce} is a random number set by the first AP, STA_{nonce} is a random number set by the STA, and "Roam Key" is a random number generated during generating PTK_{curr} using PMK_{curr}.

6. In a wireless network having at least two access points (APs), each AP having a predetermined service area, and a station (STA) that receives a communication service by associating with a first AP being one of the at least two APs, a method of supporting a roaming service for the STA at a neighbor AP of the first AP, the neighbor AP being managed by an AP-neighborhood graph drawn for the first AP, comprising the steps of:

receiving a proactive key from the first AP by proactive caching, among proactive keys generated for neighbor APs using association information gained from the association of the STA to the first AP by the first AP; and

performing fast roaming using the proactive key when the STA attempts to roam to a neighbor AP.

7. The method of claim 6, wherein the association information includes a pairwise master key (PMK: PMK_{curr}) and a roam key (RK) which are acquired at the first AP, and the MAC addresses of the STA and the neighbor APs (STA_{mac} and next AP_{mac}), and a PMK (PMK_{next}) for each of the neighbor APs is acquired using the association information and determined by

$$PMK_{next} = PRF(RK, PMK_{curr}, STA_{mac}, \text{next } AP_{mac})$$

8. The method of claim 7, wherein the RK is determined by

$$RK = PRF(PMK, \text{“Roam Key”}, AP_{nonce}, STA_{nonce})$$

where AP_{nonce} is a random number set by the first AP, STA_{nonce} is a random number set by the STA, and “Roam Key” is a random number generated during generating PTK_{curr} using PMK_{curr}.

9. In a wireless network having at least two access points (APs), each AP having a predetermined service area, and a station (STA) that receives a communication service by associating to a first AP being one of the APs, a method of supporting a roaming service between the first AP and a neighbor AP of the first AP, the neighbor AP being managed by an AP-neighborhood graph drawn for the first AP, comprising the steps of:

acquiring proactive keys for neighbor APs based on association information and transmitting the proactive keys to the neighbor APs by proactive caching, the association information being gained from the association of the STA to the first AP by the first AP; and

receiving a proactive key from the first AP and performing fast roaming using the proactive key at a neighbor AP when the STA attempts to roam to the neighbor AP.

10. The method of claim 9, wherein the association information includes a pairwise master key (PMK: PMK_{curr}) and a roam key (RK) which are acquired at the first AP, and the MAC addresses of the STA and the neighbor APs (STA_{mac} and next AP_{mac}), and a PMK (PMK_{next}) for each of the neighbor APs is acquired using the association information and determined by

$$PMK_{next} = PRF(RK, PMK_{curr}, STA_{mac}, \text{next } AP_{mac})$$

11. The method of claim 10, wherein the RK is determined by

$$RK = PRF(PMK, \text{"Roam Key"}, AP_{nonce}, STA_{nonce})$$

where AP_{nonce} is a random number set by the first AP, STA_{nonce} is a random number set by the STA, and "Roam Key" is a random number generated during generating PTK_{curr} using PMK_{curr}.

12. In a wireless network having at least two access points (APs), each AP having a predetermined service area, a station (STA) that receives a communication service by associating with a first AP being one of the at least two APs, an authentication server (AS) that authenticates the STA, and an accounting server that provides billing for the STA, a method of supporting a roaming service for the STA, comprising the steps of:

generating at the accounting server an AP-neighborhood graph for the first AP to manage neighbor APs to which the STA can move from the first AP;

notifying by the accounting server when the first AP reports to the accounting server completed association of the STA to the first AP the neighbor APs of the association;

requesting a proactive key to the AS in response to the notification from the accounting server by each of the neighbor APs;

generating a proactive key for each of the neighbor APs based on association information from the association of the STA to the first AP in response to the request and transmitting the proactive key to the neighbor AP by the AS; and

performing a pre-authentication when the STA attempts to roam to one of the neighbor APs, so that fast roaming can be carried out using the proactive key provided to the neighbor AP.

13. The method of 12, wherein the accounting server generates an AP-neighborhood graph for each of the at least two APs.

14. The method of claim 13, wherein the neighbor APs are APs within a distance less than a predetermined threshold, to which the STA can move from the first AP without being by way of any other AP.

15. The method of claim 12, wherein the association information includes a master key (MK), a pairwise master key (PMK: PMK_{curr}) assigned to the first AP, and the MAC addresses of the STA and the neighbor APs (STA_{mac} and next AP_{mac}), and a PMK (PMK_{next}) for each of the neighbor APs is acquired using the association information and determined by

$$PMK_{next} = PRF(MK, PMK_{curr}, STA_{mac}, \text{next } AP_{mac})$$